applied sciences

MDPI

Article

# Intrusion Detection with Unsupervised Techniques for Network Management Protocols over Smart Grids

**Rafael Alejandro Vega Vega [1,†], Pablo Chamoso-Santos [2,3,†], Alfonso González Briones [2,3,4,†], José-Luis Casteleiro-Roca [1,†], Esteban Jove [1,†], María del Carmen Meizoso-López [1,†], Benigno Antonio Rodríguez-Gómez [1,†], Héctor Quintián [1,†,*], Álvaro Herrero [5,†], Kenji Matsui [6,†] and Emilio Corchado [2,†] and José Luis Calvo-Rolle [1,†]**

[1] Department of Industrial Engineering, University of A Coruña, 15403 Ferrol, Spain; rafael.alejandro.vega.vega@udc.es (R.A.V.V.); jose.luis.casteleiro@udc.es (J.-L.C.-R.); esteban.jove@udc.es (E.J.); carmen.meizoso@udc.es (M.d.C.M.-L.); benigno.rodriguez@udc.es (B.A.R.-G.); jlcalvo@udc.es (J.L.C.-R.)

[2] BISITE Research Group, University of Salamanca, Edificio I+D+i, Calle Espejo 2, 37007 Salamanca, Spain; chamoso@usal.es (P.C.-S.); alfonsogb@usal.es (A.G.B.); escorchado@usal.es (E.C.)

[3] Air Institute, IoT Digital Innovation Hub (Spain), Calle Segunda 4, 37188 Salamanca, Spain

[4] Research Group on Agent-Based, Social and Interdisciplinary Applications (GRASIA), Complutense University of Madrid, 28040 Madrid, Spain

[5] Grupo de Inteligencia Computacional Aplicada (GICAP), Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad de Burgos, Av. Cantabria s/n, 09006 Burgos, Spain; ahcosio@ubu.es

[6] Faculty of Robotics & Design, Osaka Institute of Technology, Osaka 535-8585, Japan; kenji.matsui@oit.ac.jp

[*] Correspondence: hector.quintian@udc.es; Tel.: +34-881013117

[†] These authors contributed equally to this work.

Received: 14 January 2020; Accepted: 22 March 2020; Published: 27 March 2020

**Abstract:** The present research work focuses on overcoming cybersecurity problems in the Smart Grid. Smart Grids must have feasible data capture and communications infrastructure to be able to manage the huge amounts of data coming from sensors. To ensure the proper operation of next-generation electricity grids, the captured data must be reliable and protected against vulnerabilities and possible attacks. The contribution of this paper to the state of the art lies in the identification of cyberattacks that produce anomalous behaviour in network management protocols. A novel neural projectionist technique (Beta Hebbian Learning, BHL) has been employed to get a general visual representation of the traffic of a network, making it possible to identify any abnormal behaviours and patterns, indicative of a cyberattack. This novel approach has been validated on 3 different datasets, demonstrating the ability of BHL to detect different types of attacks, more effectively than other state-of-the-art methods.

**Keywords:** smart grid; computational intelligence; automatic response; exploratory projection pursuit; neural networks

## 1. Introduction

Care for the environment is not a simple trend. It is a very important matter from a legal point of view. Governments have already implemented regulations, making it compulsory to take action against environmental degradation, and there will certainly be more regulations in the future. It is necessary to remark that zero impact is impossible from a practical point of view. Nevertheless, it is necessary to pursue sustainability and to minimize impact [1]. Renewable energy systems play a very important role [2]. The environmental impact caused by this type of systems is much lesser than of conventional sources, especially when their useful life is taken into account [3].

From a theoretical point of view, depletable resources should be fully replaced by renewable energy. However, if we consider the electric sector as a global unit, our current possibilities are still too limited. In fact, several state-of-the-art studies have concluded that increasing the use of renewable energies could destabilize the energy system [4,5].

Some highly developed countries have implemented regulations that make the use of renewable energy sources obligatory, especially in new buildings. However, the connection of those buildings to the power network makes energy management very difficult. This is because, even when they generate energy that is not electricity, they can still cause the energy demand to reduce.

The main problem of the electric sector is that the levels of energy production must be equivalent to the amount of energy being consumed [6]. This justifies the need for energy storage systems which mitigate problems associated with unbalanced generation and consumption levels [7]. Thanks to this kind of system, when excess energy is generated, the excess consumption can be stored, similarly, when the energy needs are greater than the amount of generated energy, the storage system may supply the required energy. The main problem currently is that energy storage systems are inefficient [8].

Considering the problems described above, the optimal management of every part of the power network is mandatory. However, to make efficient management possible, it is necessary to develop adequate tools that will ensure the correct performance of the system as a whole [9]. The term Smart Grid [9,10] emerged as an answer to all the issues described above. The Smart Grid makes it possible to measure the levels of energy generation/consumption and forecast the future levels of both variables, making it possible to manage the entire system more effectively. Nevertheless, the task of precisely adjusting energy generation to demand continues to be very complex, thus, it is preferable to use an energy storage system [7].

From a global context, a smart grid can be defined as the dynamic integration of developments in electrical engineering and energy storage, the advances in information and communication technologies (or ICT), their implementation in the electricity-related processes (generation, transport, distribution, storage and marketing, including alternative energy) [11]. ICT makes it possible to concatenate security, control, instrumentation, measurement, quality and administration of energy, etc., in a single management system, with the primary objective of making efficient and rational use of electricity [12].

The concept described above could also include the integration of other actors in the area of measurement and control, such as gas sources and water services. Thus, smart electricity networks become part of a macro-concept of territorial dominance, such as that of smart cities [13]. The smart grid is a type of efficient electricity management that uses computer technology to optimize the production and distribution of electricity, in order to achieve a greater balance between supply and demand, as well as producers and consumers [11].

The smart grid must be protected from all types of vulnerabilities, like natural disasters, and of course, it must be robust against attacks [14]. Security is essential because otherwise the information flow between all the actors would not be reliable [15]. In consequence, the smart grid concept would fail completely [16]. Robust communications and the reliability of the information must be guaranteed in all cases for satisfactory smart grid performance [12,14].

Among the actors in the Smart Grid, there are three crucial components to which special attention should be paid [9]: data acquisition, data management and communications. It is necessary to ensure secure communications and the reliability of the available data. Moreover, protection mechanisms must be implemented for protection against any type of attack. The above-mentioned goals may be achieved thanks to advances in cybersecurity [17].

Cybersecurity has become a relevant field in multiple areas and it is the basis of the proposed solution.

The main objective of this research is to identify cyberattacks which produce anomalous behaviours in network management protocols. This has been made possible through the use of a novel neural projectionist technique called Beta Hebbian Learning (BHL), which provides a visual representation of the network traffic and detects abnormal network behaviours and patterns, indicative of a cyberattack.

The rest of the paper is structured as follows: Section 2 presents a review of sate-of-the-art research in the field. Section 3 describes the main materials and methods used in this research, including the datasets, and the novel Beta Hebbian Learning algorithm used for attack detection. The next section details the results of each of the experiments performed on the real datasets, and finally, Section 5 presents the conclusions.

## 2. Literature Review

This section presents related state-of-the-art literature and the principal advantages of the proposed model.

Several authors carried out research on building a system for real-time intrusion detection by training it with a dataset.

However, current systems are only able to detect some but not all the indications of an intrusion. This is because they are not able to monitor all the behaviours in the network On the contrary, projectionist techniques are able to provide a visual overview of the network traffic. Earlier dimensionality reduction techniques were applied to visualize network data using scatter plots [18–23].

In the case of [24], several projectionist algorithms, such as PCA, CMLHL, CCA, and SOM network, have been applied to monitor the traffic of the Euskalert network (Honeynet data) [25], to discover behaviour and strategies indicative of an attack. In [26], the same techniques have been applied to GICAP-IDS and DARPA datasets [27], and their performance has been measured according to different variables, such as data volume, system dynamics and network traffic diversity, including first-time attacks (0-day). Then, the authors presented a novel Multi-Agent System which combined Artificial Neural Networks (ANN) with Case-Based Reasoning (CBR) techniques for the detection of attacks in computer networks [28]. This new IDS, known as RT-MOVICABIDS, has been validated using three different datasets. Those datasets have also been used in our study, as described further on in the article. In [29], clustering and visualization techniques have been combined to generate an automatic response to the previously developed MOVICAB-IDS system. The modified MOVICAB-IDS has been applied to the three datasets, to assess the improvement of the proposed approach. Furthermore, in [30], it has been validated using a community search dataset. This type of attack involves guessing the password, it has been detected by MOVICAB-IDS, which demonstrated to perform better than other well-know algorithms for detecting attacks on continuous network flow.

Finally, in [31], MOVICAB-IDS has been applied to a dataset that contained flow-based information (14.2 M flows). The University of Twente [32] collected this information in September 2008, using a honeypot.

More recently, a novel EPP algorithm, BHL, has been applied to Android malware families [33,34], obtaining much better results than other well-known algorithms.

BHL has also been previously employed in the analysis of the internal structure of a series of datasets [35,36], providing a clear projection of the original dataset. More specifically, it has been successfully applied to Android malware datasets [33,34], where its task was to characterize Android malware families. Therefore, this research aims to apply BHL to the datasets that have previously been used by MOVICAB-IDS, with the aim of improving the obtained projections and achieving a better visual representation of the network traffic. This facilitates the early identification of anomalous situations which may be indicative of a cyberattack in the computer network.

## 3. Materials and Methods

In this research, the Exploratory Projection Pursuit (EPP), called Beta Hebbian Learning algorithm (BHL) [37], has been employed. It is based on beta distribution and has been applied to 3 real datasets in order to assess its ability to detect anomalous situations in the network management protocol. Its performance has been compared with the results obtained by the MOVICAB-IDS algorithm [29].

### *3.1. Preprocessing*

Before using the obtained dataset, they had to undergo a preprocessing stage. First, all missing values were removed.

Outliers have been removed in order to prevent them from being identified as intrusion samples, as this would have affected the training process. Considering as outliers the samples with values outside the $\mu \pm 5\sigma^2$ range, where $\mu$ is the average and $\sigma^2$ is the variance.

The application of this criterion may lead to a situation where some outliers could be considered as intrusion samples. However, their influence on the training process would be insignificant, given that their degree of deviation from the mean would have been small. Although once the system is trained these extreme outliers could be identified as intrusions, a real intrusion is never considered as normal behaviour due to the influence of the outliers during the training process.

Finally a normalization of each variable between the range -1 to 1 has been applied to ensure the stability of the BHL network during the training process [37].

### *3.2. Beta Hebbian Learning Algorithm*

Artificial Neural Networks (ANN) are typically software simulations that emulate some of the features of real neural networks found in the animal brain. Among the range of applications of unsupervised artificial neural networks, data projection or visualization is the one that facilitates, human experts, the analysis of the internal structure of a dataset. This can be achieved by projecting data on a more informative axis or by generating maps that represent the inner structure of datasets. This kind of data visualization can usually be achieved with techniques such as Exploratory Projection Pursuit (EPP) [37,38] which project the data onto a low dimensional subspace, enabling the expert to search for structures through visual inspection.

The Beta Hebbian Learning technique (BHL) [31] is an Artificial Neural Network belonging to the family of unsupervised EPP, which uses Beta distribution as part of the weight update process, for the extraction of information from high dimensional datasets by projecting the data onto low dimensional (typically 2 dimensional) subspaces. This technique is better than other exploratory methods in that it provides a clear representation of the internal structure of data.

The Beta Hebbian Learning network is based on a Negative Feedback Network, therefore to introduce it, consider an N-dimensional input vector, $x$, and a M-dimensional output vector, $y$, where $W_ij$ is the weight linking input $j$ to output $i$ and let $\eta$ be the learning rate.

The initial situation is that there is no activation at all in the network. The input data is feedforward via weights from the input neurons (the x-values) to the output neurons (the y-values), where a linear summation is performed to activate the output neuron (see Figure 1). This is expressed by Equation (1).

$$y_i = \sum_{j=1}^{N} W_{ij} x_j, \forall i \tag{1}$$

The activation is feedback through the same weights and is subtracted from the inputs (see Equation (2)).

$$Feedback : e_j = x_j - \sum_{i=1}^{M} W_{ij} y_i \tag{2}$$

After that, simple Hebbian learning is performed between input and outputs, the weight update is obtained by means of Equation (3).

$$\Delta W_{ij} = \eta e_j y_i \tag{3}$$

The effect of the negative feedback is to stabilize the learning in the network. For this reason, it is not necessary to normalize or clip the weights to achieve a stable solution.

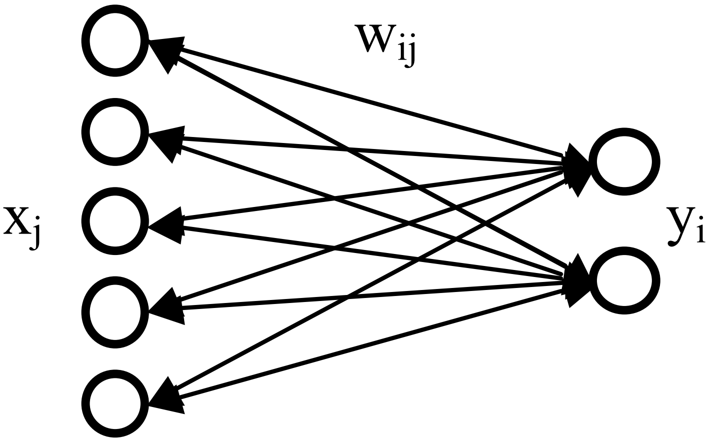

**Figure 1.** Basic architecture of a negative feedback network.

Note that this algorithm is clearly equivalent to Oja's Subspace Algorithm (Equation (4)).

$$\Delta W_{ij} = \eta (x_j - \sum_{i=1}^{M} W_{ij} y_i) y_i \tag{4}$$

This network is capable of finding the principal components of the input data in a manner that is equivalent to Oja's Subspace algorithm. Thus, it may be said that the network uses simple Hebbian learning to enable the weights to converge and extract the maximum content from the input data.

Since the model is equivalent to Oja's Subspace algorithm, we might legitimately ask what we gain by using the negative feedback in this way.

Writing the algorithm in this way, gives a model of the process which allows to devise different versions and algorithms like the Beta Hebbian Learning rule. This rule is based on an explicit view of the residual which is never independently calculated using e.g., Oja's learning rule.

A general cost function associated with the Beta Hebbian Learning network can be denoted as Equation (5)

$$J = E(-p(e)) \tag{5}$$

where $E$ is the expected value operator.

Therefore, the gradient descent J is presented in Equation (6).

$$\Delta W \propto -\frac{\partial J}{\partial W} = -\frac{\partial J}{\partial e}\frac{\partial e}{\partial W} \tag{6}$$

Thus, the optimal cost function can be obtained if the PDF of the residuals is known. Therefore, the residual ($e$) can be expressed by Equation (7) in terms of Beta distribution parameters ($B(\alpha, \beta)$):

$$p(e) = e^{\alpha-1}(1-e)^{\beta-1} = (x - Wy)^{\alpha-1}(1 - x + Wy)^{\beta-1} \tag{7}$$

where $\alpha$ and $\beta$ control the PDF shape of the Beta distribution, $e$ is the residual, $x$ are inputs of the network, $W$ is the weight matrix, and $y$ is the output of the network.

Finally, gradient descent can be used to maximize the likelihood of the weights (Equation (8)):

$$
\begin{aligned}
\Delta W \propto \frac{\partial p_i}{\partial W_{ij}} = \frac{\partial}{\partial W_{ij}}[(x_j - W_{ij}yi)^{\alpha-1}(1 - x_j + W_{ij}y_i)^{\beta-1}] &= \\
[(\alpha-1)(x_j - W_{ij}yi)^{\alpha-2}(-y_i)(1 - x_j + W_{ij}y_i)^{\beta-1}] &+ \\
[(x_j - W_{ij}y_i)^{\alpha-1}(\beta-1)(1 - x_j + W_{ij}yi)^{\beta-2}y_i] &= \\
[(\alpha-1)e_j^{\alpha-2}(-y_i)(1-e_j)^{\beta-1}] + [e_j^{\alpha-1}(\beta-1)(1-e_j)^{\beta-2}y_i] &= \\
y_i e_j^{\alpha-2}[(\alpha-1)(-1)(1-e_j)^{\beta-1} + e_j(\beta-1)(1-e_j)^{\beta-2}] &= \\
y_i e_j^{\alpha-2}(1-e_j)^{\beta-2}[(\alpha-1)(-1)(1-e_j) + e_j(\beta-1)] &= \\
y_i e_j^{\alpha-2}(1-e_j)^{\beta-2}[(-\alpha + e_j\alpha + 1 - e_j + e_j\beta - e_j)] &= \\
y_i e_j^{\alpha-2}(1-e_j)^{\beta-2}[(e_j(\alpha+\beta-2) + 1 - \alpha)] &
\end{aligned}
\tag{8}
$$

Therefore, a BHL architecture can be expressed by means the following equations:

$$
Feedforward : y_i = \sum_{j=1}^{N} W_{ij}x_j, \forall i \tag{9}
$$

$$
Feedback : e_j = x_j - \sum_{i=1}^{M} W_{ij}y_i \tag{10}
$$

$$
Weightsupdate : \Delta W_{ij} = \eta(e_j^{\alpha-2}(1-e_j)^{\beta-2}(1 - \alpha + e_j(\alpha+\beta-2)))y_i \tag{11}
$$

where $\eta$ is the learning rate.

For the final implementation of the algorithm, the absolute vale of the error where used and finally the sign operator where added to the final result in the weights update.

### 3.3. Dataset

In this research, BHL has been applied to 3 real datasets. Each dataset consists of the monitorization of simple networks where different anomalous situations occur. The dataset analyzed in present research has been generated in a small-size university network.

In all cases, the same 5 variables were monitored:

- Packet ID.
- Timestamp: respect to the first captured packet.
- Source Port: It is the host port from which the packet is sent.
- Destination Port: It is the host port to which the packet is sent.
- Packet Size.
- Protocol ID: from 1 to 35 for different packet protocols.

Each dataset contains the data that had been collected during the monitoring of a network in a period where a specific attack occured. The type of attack is different in each dataset. A small part of the data is captured for analysis.Consequently, only the above-mentioned 5 fields of packet headers are used [23], and one output variable is only used to show the real category (normal and attack) but it is never used for training.

## 4. Experiments and Results

The BHL algorithm is applied as a clustering technique to identify the internal structure of the 3 datasets and any anomalous situations present in each one. As, the dataset condition in a great manner the selection of optimal parameters, different values combinations of $\alpha$ and $\beta$ parameters were tried and the best combination was selected (Table 1). Once the best parameters were obtained, several runs with random weights initialization were performed for validating the repeatability of the obtained results.

**Table 1.** Dataset description.

| Dataset | Description | N° Samples | N° of Attacks |
|---|---|---|---|
| 1 | Type of attack: Scans. In this type of attack, diverse messages are sent to various host ports to extract information about the activity status. An external agent could send these messages with the aim of getting information about host network services. However, in the case of a network scan, the target of several hosts is a specific port (frequently, a single IP address range for all hosts). The target port numbers are 161, 162, and 3750 in the same IP address range for all machines. | 866 | 18 attacks × 3 ports = 54 attacks |
| 2 | Type of attack: MIB (management information base) Information Transfer. In this attack part of the information (or all) of SNMP MIB is captured, usually by means of get/get-bulk command, which represents a potentially dangerous situation. However, some queries of MIB could belong to a "normal" network behavior. | 5000 | 226 attacks |
| 3 | Type of attack: It is a combination of Scan and MIB Information Transfer. | 5866 | 18 attacks × 3 ports = 54 port attacks and 226 MIB attacks |

In the case of the k-means algorithm, to ensure good results in the creation of the cluster, the k-means algorithm was random initialization of the centroids, and the training was repeated 20 times. These repetitions allow avoiding to finish the training in a local minimum.

In all cases, Matlab software was used to analyze the 3 datasets with both algorithms. The implmentation of BHL was done according to previous researches [37] and the Matlab version of the k-means algorithm was used.

Table 2 shows the best combination of parameters and Figures 1–6 the projections for each dataset and algorithm (BHL and k-means).

**Table 2.** BHL and k-means parameters for datasets 1, 2 and 3.

| Algorithm | Parameters |
|---|---|
| BHL (dataset 1) | iters = 3000, lrate = 0.01, $\alpha = 3$, $\beta = 3$ |
| BHL (dataset 2) | iters = 10,000, lrate = 0.01, $\alpha = 3$, $\beta = 4$ |
| BHL (dataset 3) | iters = 10,000, lrate = 0.05, $\alpha = 3.5$, $\beta = 5$ |
| k-means (dataset 1, 2 and 3) | k = 6, random initialization of the centroids, sqEuclidean distance |

The axes of BHL projections correspond to the first two components of the new subspace (as non-linear combinations of the original space), which do not have any meaning or direct relationship with the variables of the original dataset.

Figure 2, shows the best projection of BHL for dataset 1, it shows that BHL can clearly identify 3 clusters which correspond to each scan port attack (port numbers 161, 162, and 3750).

Figure 3 shows the results obtained in past researches. It can be observed that, like BHL, there also were 3 clusters in the results, which correspond to different types of scan port attacks. Therefore, due to the simplicity of this dataset, it is not possible to get better results, and in all cases, the scan port attack can be identified easily (k-means clustering was applied to the projected data representation).

Nevertheless, in the case of dataset 2, the are significant differences. In the case of BHL, its projection shows a clear distinction between a normal (green crosses Figure 4), and an abnormal situation (MIB transfer source-destination, red dots in Figure 5). In the case of MOVICAB-IDS, the final projection mixes both classes (normal and attack), in different clusters (see Figure 5).

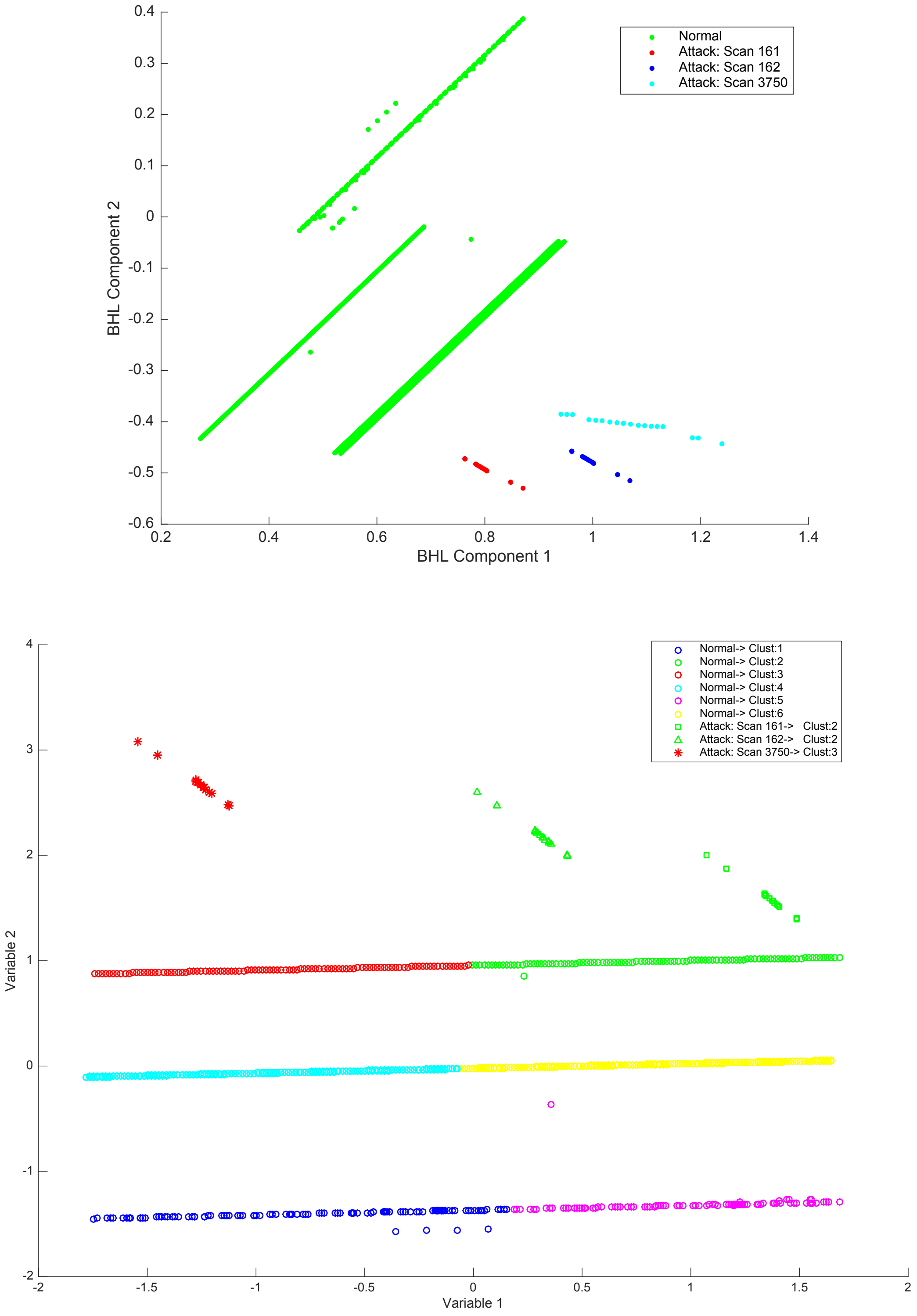

**Figure 3.** MOVICAB projection for dataset 1, port scan attack.

Finally, dataset 3 presents a combination of 2 types of attacks, scan port (3 port attacks) and MIB transfer (source-destination and destination-source attacks), therefore, there are 5 attacks and the rest of the sample contains information about the normal behaviour of the network. Figure 6 presents the best BHL projection for dataset 3 (MIB transfer and scan port). In this case, BHL can clearly differentiate between the samples associated with normal network behaviour (green samples in Figure 6) and the samples belonging to abnormal situations. Moreover, BHL can distinguish the different types of scan port (red, blue and cyan samples in Figure 6) and MIB transfer attacks (2 types, yellow and magenta samples in Figure 6).

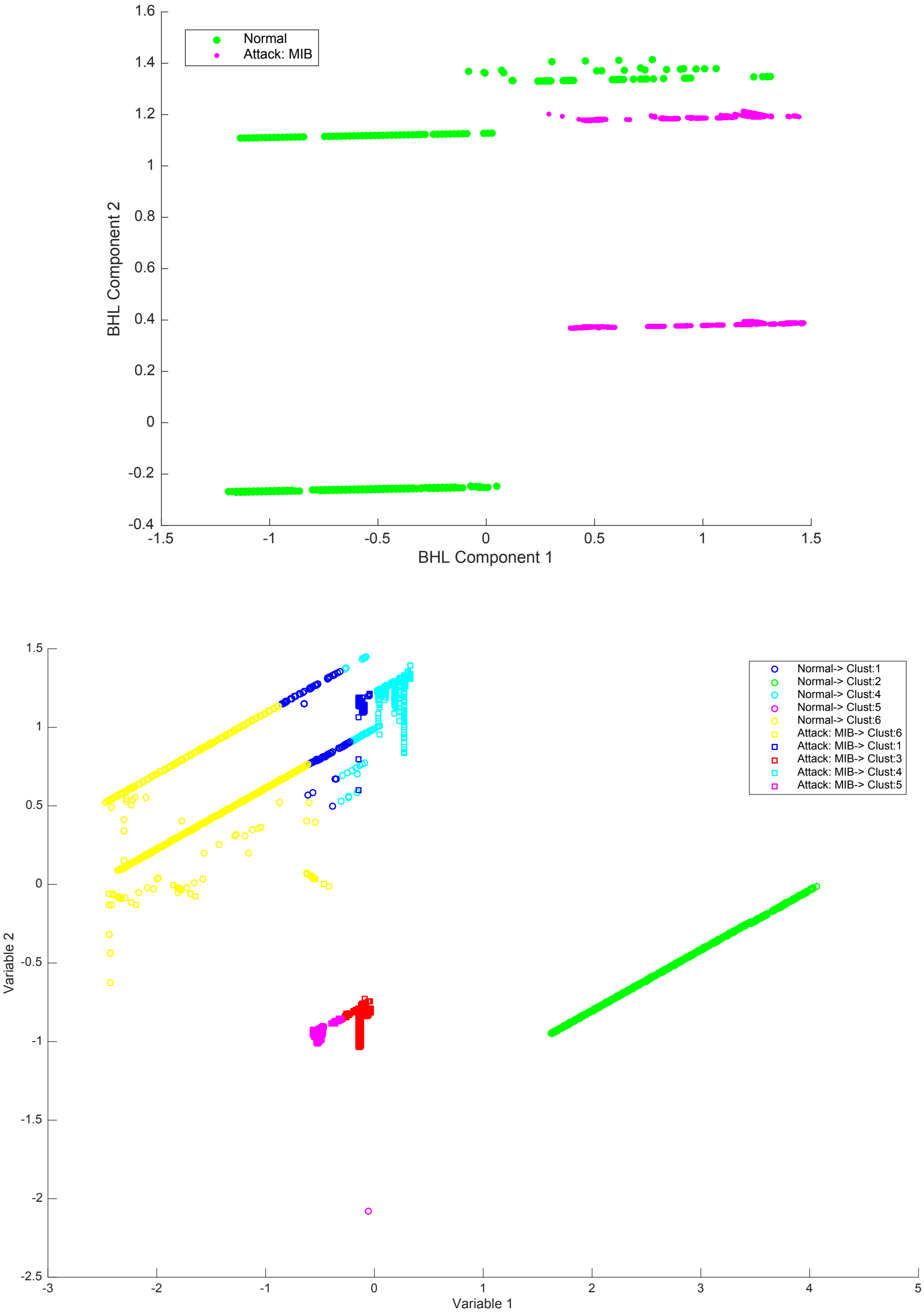

**Figure 5.** MOVICAB projection for dataset 2, MIB transfer attack.

However, in previous researches (see Figure 7), MOVICAB-IDS was not able to generate separate groups without mistakes, as it mixed packets belonging to different categories, failing to distinguish between normal and abnormal samples. It is important to remark, that MOVICAB-IDS was able to detect 3 classes; normal samples, scan port, and MIB, however, it was not able to distinguish between the different types of attacks; as can be seen in Figure 7, it confused MIB transfer with normal samples. On the contrary, BHL is able to clearly distinguish between all the types of attacks, including destination-source and source-destination MIB transfer attacks.

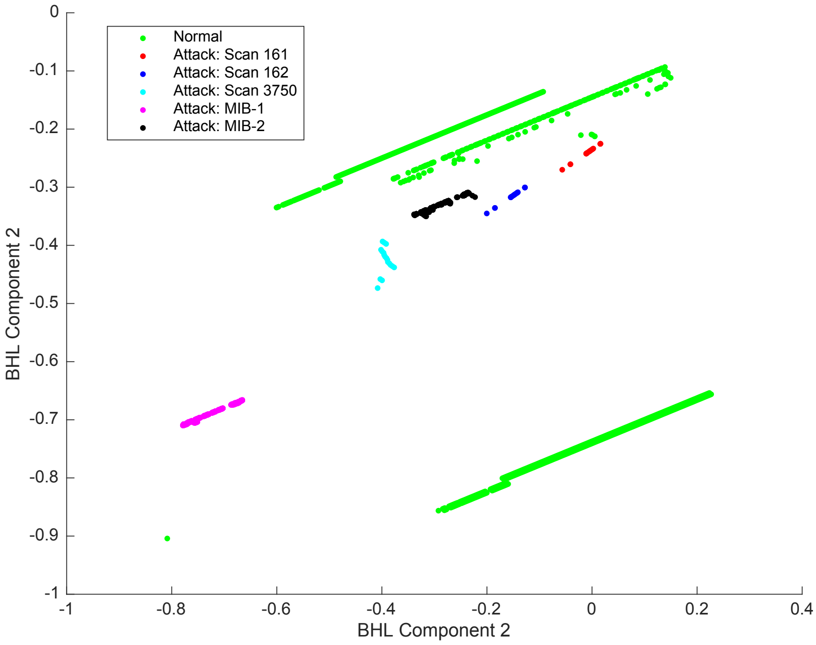

**Figure 6.** BHL projection for dataset 3, MIB transfer and port scan attacks.

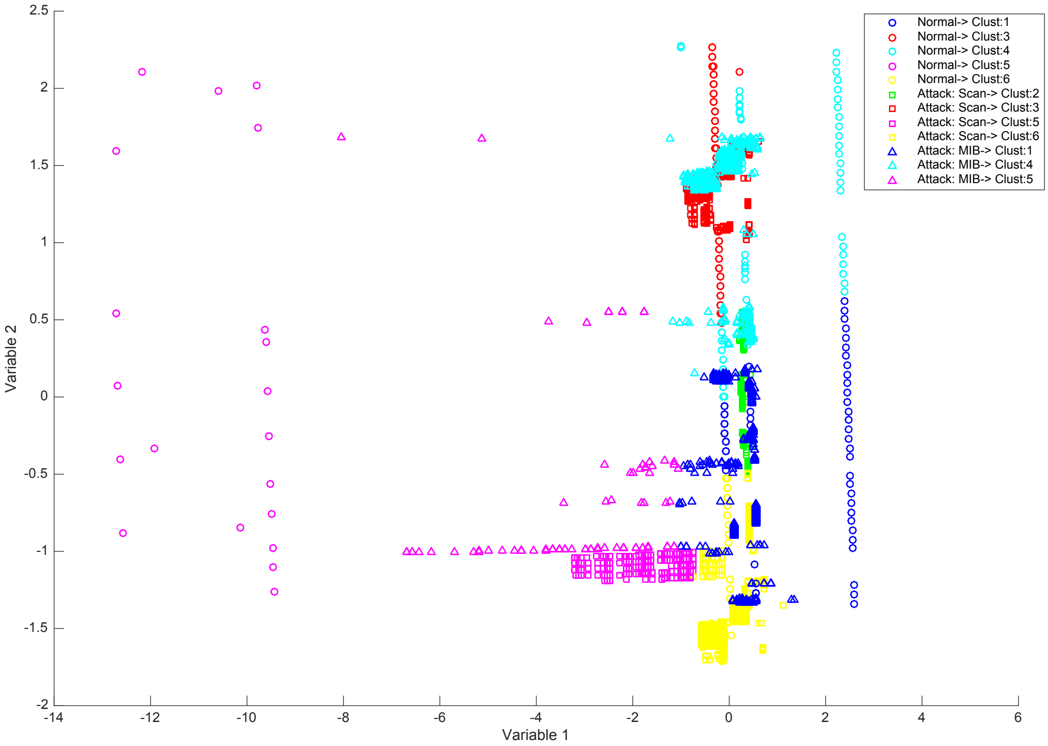

**Figure 7.** MOVICAB projection for dataset 3, MIB transfer and port scan attacks.

## 5. Conclusions

The increase in data traffic in smart grids makes them increasingly vulnerable to cyberattacks. Having the tools that permit the correct analysis and visualization of data traffic in these networks becomes increasingly important. Therefore, the use of tools that are capable of visually representing the general behavior of these networks (in terms of data traffic), allows to quickly and easily detect possible attacks that cause abnormal network behavior.

The results presented in Section 4 demonstrate that Dimensional Reduction Techniques (DRT), provide a general overview of the internal dataset structure. This helps prevent potential cyberattacks in smart grids through the visual inspection of the network's traffic data.

The previously applied DRTs were able to visually represent the behaviour of the network's traffic data, however, their clustering is not good enough, especially in the case of different types of attacks that are produced at the same time (MIB and Scan port).

On the contrary, BHL gives a detailed overview of the network traffic and provides well-defined clusters that make it possible to identify anomalous situations and different types of attacks, overcoming the challenges associated with data volume, system dynamics and network traffic diversity, including first-time attacks (0-day).

The clarity of BHL projections makes it easy to distinguish between normal traffic and anomalous traffic patterns, facilitating the early detection of attacks. BHL can easily identify scan port attacks at different ports. Moreover, when this type of attack is combined with the MIB attack, BHL is not only able to distinguish between them but also between the two types of MIB attack and the scanned ports. This makes BHL a powerful tool for network management protocols.

The results of the conducted experiment have proven that BHL's performance is superior to that of the techniques used in previous researches, proving comprehensible projections, where attacks are clearly distinguished from the normal behaviour of the network, even when different types of attacks occur at the same time.

The results obtained by EPP algorithms such as BHL demonstrate that they are suitable to be applied in smart grids for the detection of intrusions in the network. In conclusion, advances have been made in the early identification and characterization of cyberattacks. However, there is still a lot of room for improvement, especially in relation to the security of Smart Grids.

**Author Contributions:** Data curation, R.A.V.V. and H.Q.; Investigation, H.Q. and J.-L.C.-R.; Methodology, P.C.-S., A.G.B. and H.Q.; Project administration, M.d.C.M.-L. and B.A.R.-G.; Software, R.V.V. and E.J.; Supervision, J.L.C.-R., A.H., K.M. and E.C.; Validation, H.Q. and R.V.V.; Writing, original draft, R.V.V. and P.C.-S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Acknowledgments:** TEACHING STAFF MOBILITY UNDER BILATERAL AGREEMENTS (University of Salamanca—Osaka Institute of Technology 2019).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Kuwae, T.; Hori, M. Global Environmental Issues. In *Blue Carbon in Shallow Coastal Ecosystems: Carbon Dynamics, Policy, and Implementation*; Routledge: London, UK, 2019.
2. Karunathilake, H.; Hewage, K.; Mérida, W.; Sadiq, R. Renewable energy selection for net-zero energy communities: Life cycle based decision making under uncertainty. *Renew. Energy* **2019**, *130*, 558–573. [CrossRef]
3. Prakash, R.; Bhat, I.K. Energy, economics and environmental impacts of renewable energy systems. *Renew. Sustain. Energy Rev.* **2009**, *13*, 2716–2721.
4. Chen, S.; Zhu, F.; Long, H.; Yang, J. Energy footprint controlled by urban demands: How much does supply chain complexity contribute? *Energy* **2019**, *183*, 561–572, doi:10.1016/j.energy.2019.06.167. [CrossRef]
5. Carrosio, G.; Scotti, I. The 'patchy' spread of renewables: A socio-territorial perspective on the energy transition process. *Energy Policy* **2019**, *129*, 684–692, doi:10.1016/j.enpol.2019.02.057. [CrossRef]
6. Montero-Sousa, J.A.; Casteleiro-Roca, J.L.; Calvo-Rolle, J.L. Evolution of the electricity sector after the 2nd world war. *DYNA* **2017**, *92*, 280–284.

7. Nizami, M.; Haque, A.; Nguyen, P.; Hossain, M. On the application of Home Energy Management Systems for power grid support. *Energy* **2019**, *188*, 116104, doi:10.1016/j.energy.2019.116104. [CrossRef]
8. Yang, C.J.; Jackson, R.B. Opportunities and barriers to pumped-hydro energy storage in the United States. *Renew. Sustain. Energy Rev.* **2011**, *15*, 839–844. [CrossRef]
9. Amin, M. Smart Grid. In *Public Utilities Reports*; Public Utilities Fortnightly: Rochester, NY, USA, 2015.
10. De Souza Dutra, M.D.; Anjos, M.F.; Digabel, S.L. A general framework for customized transition to smart homes. *Energy* **2019**, *189*, 116138, doi:10.1016/j.energy.2019.116138. [CrossRef]
11. Yu, Y.; Luan, W. Smart grid and its implementations. *Proc. CSEE* **2009**, *29*, 1–8.
12. Gungor, V.C.; Sahin, D.; Kocak, T.; Ergut, S.; Buccella, C.; Cecati, C.; Hancke, G.P. Smart grid technologies: Communication technologies and standards. *IEEE Trans. Ind. Inform.* **2011**, *7*, 529–539. [CrossRef]
13. Moslehi, K.; Kumar, R. A reliability perspective of the smart grid. *IEEE Trans. Smart Grid* **2010**, *1*, 57–64. [CrossRef]
14. McDaniel, P.; McLaughlin, S. Security and privacy challenges in the smart grid. *IEEE Secur. Priv.* **2009**, *7*, 75–77. [CrossRef]
15. Khurana, H.; Hadley, M.; Lu, N.; Frincke, D.A. Smart-grid security issues. *IEEE Secur. Priv.* **2010**, *8*, 81–85. [CrossRef]
16. Metke, A.R.; Ekl, R.L. Security technology for smart grid networks. *IEEE Trans. Smart Grid* **2010**, *1*, 99–107. [CrossRef]
17. Leszczyna, R. A review of standards with cybersecurity requirements for smart grid. *Comp. Secur.* **2018**, *77*, 262–276, doi:10.1016/j.cose.2018.03.011. [CrossRef]
18. Wagner, M.; Fischer, F.; Luh, R.; Haberson, A.; Rind, A.; Keim, D.A.; Aigner, W. A Survey of Visualization Systems for Malware Analysis. In Proceedings of the Eurographics Conference on Visualization (EuroVis)—STARs, Cagliari, Italiy, 25–29 May 2015; doi:10.2312/eurovisstar.20151114. [CrossRef]
19. González, A.; Herrero, Á.; Corchado, E. Neural Visualization of Android Malware Families. In Proceedings of the International Joint Conference SOCO'16-CISIS'16-ICEUTE'16, San Sebastián, Spain, 19–21 October 2016; pp. 574–583, doi:10.1007/978-3-319-47364-2_56. [CrossRef]
20. Paturi, A.; Cherukuri, M.; Donahue, J.; Mukkamala, S. Mobile malware visual analytics and similarities of Attack Toolkits (Malware gene analysis). In Proceedings of the International Conference on Collaboration Technologies and Systems (CTS), San Diego, CA, USA, 20–24 May 2013; pp. 149–154, doi:10.1109/CTS.2013.6567221. [CrossRef]
21. Park, W.; Lee, K.; Cho, K.; Ryu, W. Analyzing and detecting method of Android malware via disassembling and visualization. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC), Busan, Korea, 22–24 October 2014; pp. 817–818, doi:10.1109/ICTC.2014.6983300. [CrossRef]
22. Moonsamy, V.; Rong, J.; Liu, S. Mining permission patterns for contrasting clean and malicious android applications. *Future Gener. Comp. Syst.* **2014**, *36*, 122–132, doi:10.1016/j.future.2013.09.014. [CrossRef]
23. Somarriba, O.; Zurutuza, U.; Uribeetxeberria, R.; Delosieres, L.; Nadjm-Tehrani, S. Detection and Visualization of Android Malware Behavior. *J. Electr. Comp. Eng.* **2016**, *2016*, 17,doi:10.1155/2016/8034967. [CrossRef]
24. Herrero, Á.; Zurutuza, U.; Corchado, E. A Neural-Visualization IDS for Honeynet Data. *Int. J. Neural Syst.* **2012**, *22*, 1250005, doi:10.1142/S0129065712500050. [CrossRef]
25. Basque Honeypot Network. Euskalert. 2010. Available online: https://www.eurekalert.org/ (accessed on 10 May 2010).
26. Corchado, E.; Herrero, Á. Neural visualization of network traffic data for intrusion detection. *Appl. Soft Comput.* **2011**, *11*, 2042–2056, doi:10.1016/j.asoc.2010.07.002. [CrossRef]
27. Lincoln Laboratory, M.I.o.T. 2000 DARPA Intrusion Detection Scenario Specific Datasets. 2019. Available online: https://www.ll.mit.edu/r-d/datasets/2000-darpa-intrusion-detection-scenario-specific-datasets (accessed on 3 December 2019).
28. Herrero, Á.; Navarro, M.; Corchado, E.; Julián, V. RT-MOVICAB-IDS: Addressing real-time intrusion detection. *Future Gener. Comp. Syst.* **2013**, *29*, 250–261, doi:10.1016/j.future.2010.12.017. [CrossRef]
29. Sánchez, R.; Herrero, Á.; Corchado, E. Visualization and Clustering for SNMP Intrusion Detection. *Cybernet. Syst.* **2013**, *44*, 505–532, doi:10.1080/01969722.2013.803903. [CrossRef]
30. Sánchez, R.; Herrero, Á.; Corchado, E. Clustering extension of MOVICAB-IDS to identify SNMP community searches. *Log. J. IGPL* **2015**, *23*, 121–140, doi:10.1093/jigpal/jzu035. [CrossRef]

31. Sánchez, R.; Herrero, Á.; Corchado, E. Clustering extension of MOVICAB-IDS to distinguish intrusions in flow-based data. *Log. J. IGPL* **2017**, *25*, 83–102, doi:10.1093/jigpal/jzw047. [CrossRef]
32. Sperotto, A.; Sadre, R.; van Vliet, F.E.; Pras, A. A Labeled Data Set for Flow-Based Intrusion Detection. In Proceedings of the Operations and Management, 9th IEEE International Workshop (IPOM 2009), Venice, Italy, 29–30 October 2009; pp. 39–50, doi:10.1007/978-3-642-04968-2_4. [CrossRef]
33. Vega Vega, R.; Quintián, H.; Calvo-Rolle, J.L.; Herrero, Á.; Corchado, E. Gaining deep knowledge of Android malware families through dimensionality reduction techniques. *Log. J. IGPL* **2019**, *27*, 160–176, doi:10.1093/jigpal/jzy030. [CrossRef]
34. Vega, R.V.; Quintián, H.; Cambra, C.; Basurto, N.; Herrero, Á.; Calvo-Rolle, J.L. Delving into Android Malware Families with a Novel Neural Projection Method. *Complexity* **2019**, *2019*, 10,doi:10.1155/2019/6101697. [CrossRef]
35. Jove, E.; Casteleiro-Roca, J.L.; Quintián, H.; Pérez, J.A.M.; Calvo-Rolle, J.L. A fault detection system based on unsupervised techniques for industrial control loops. *Expert Syst.* **2019**, *36*, e12395, doi:10.1111/exsy.12395. [CrossRef]
36. Jove, E.; Casteleiro-Roca, J.L.; Quintián, H.; Pérez, J.A.M.; Calvo-Rolle, J.L. A New Approach for System Malfunctioning over an Industrial System Control Loop Based on Unsupervised Techniques. In Proceedings of the International Joint Conference SOCO'18-CISIS'18-ICEUTE'18, San Sebastián, Spain, 6–8 June 2018; pp. 415–425, doi:10.1007/978-3-319-94120-2_40. [CrossRef]
37. Quintián, H.; Corchado, E. Beta Hebbian Learning as a New Method for Exploratory Projection Pursuit. *Int. J. Neural Syst.* **2017**, *27*, 1–16, doi:10.1142/S0129065717500241. [CrossRef]
38. Berro, A.; Larabi Marie-Sainte, S.; Ruiz-Gazen, A. Genetic algorithms and particle swarm optimization for exploratory projection pursuit. *Ann. Math. Artif. Intell.* **2010**, *60*, 153–178, doi:10.1007/s10472-010-9211-0. [CrossRef]